Intel® Wired for Management (WfM) Self-Test ToolKit Version 2.0-4 Readme File

Feburary 7, 2000

“Year 2000 Capable”

An Intel® product, when used in accordance with its associated documentation, is "Year 2000 Capable" when, upon installation, it accurately stores, displays, processes, provides, and/or receives date data from, into, and between 1999 and 2000, and the twentieth and twenty-first centuries, including leap year calculations, provided that all other technology used in combination with said product properly exchanges date data with it. Intel® makes no representation about individual components within the product should they be used independently from the product as a whole.

This Readme file supplements the individual product documents included in this release.

CONTENTS

PART 7: COMMON QUESTIONS

PART 1: INSTALLATION

Execute the file wfmst20.exe to install the Self-Test tools. This is a self-extracting executable and it will guide you through the steps necessary to complete the installation of all components. You can install only the documentation by clearing all components or de-selecting all components except for the documentation and then completing the install. Note that only the base Self Test Toolkit documentation will be installed. Documentation for a specific tool is only installed when the tool is selected for installation.

Please un-install any previous versions of the self test kit before installing the updated toolkit. Problems may occur otherwise.

Some of the tools in this kit have dependencies on other tools or components. See the document "Self Test Documentation" under the program folder "Program Files\Intel\WFM_Self_Test for more details.

PART 2: TECHNICAL SUPPORT PROCEDURES

Intel® Wired for Management (WfM) Self-Test Version 2.0-4 support contact information

Problems with installation and operation of the Self-Test ToolKit should be reported to:

ial.support@intel.com

The Distributed Management Task Force, Inc (DMTF) provides documents, files and industry specification support for members through their World Wide Web home page. As the Desktop Management Interface (DMI) technology grows and develops, announcements and updates are distributed through these points of contact.

World Wide Web site: http://www.dmtf.org

Internet FTP site: ftp.dmtf.org

Free electronic copies of the DMI specification and updated reference MIF files containing the latest revisions of DMTF-approved Standard Groups may also be obtained.

This information was current and correct at the time this product was released.

PART 3: GENERAL INFORMATION

This release of the Intel® Wired for Management Self-Test Kit, Version 2.0-4 includes several tools that allow the user to test if Wired For Management V2.0 is enabled. There is a "Common Questions" section in PART 7 of this readme file to assist developers in understanding the new tools and technologies. Questions are derived from actual questions submitted to the Wired for Management engineering support team.

A new Remote Lockout tool is supplied for testing version 1.1 remote lockout implementations. This revision became part of the WfM 2.0 baseline on 10/15/99 and is a required element for WfM 2.0 enabled systems.

The Preboot Execution Environment (PXE) Product Development Kit (PDK) V3.0, build 078 provides the latest bug fixes. Note that this release requires the use of the latest Adobe* Acrobat reader. This may be obtained from Adobe's site for free.

The Boot Integrity Services or BIS Self-Test tool is now part of the WfM 2.0-4 Self-Test Toolkit. This tool verifies the existence of BIS on a platform and performs a limited functionality check of the BIS API. See the accompanying documentation for details.

The DCTS2.EXE test tool now part of the WfM Self-Test Toolkit allows users to view DMI 2.0 information from a remote system and monitor events generated by DMI instrumentation.

V1.01 of the System Management BIOS (SMBIOWFM.EXE) tool provides functionality to view structures above 1 MB. Please see PART 4 of this document for details and refer to the supporting documentation supplied with each of the tools for more information.

The Remote Wake-up tool has been updated to v0.4. A bug fix was implemented to fix a seldom seen Dr. Watson error when positioning the dialog boxes.

The un-install facility provided with the Intel® Wired for Management Self-Test Version 2.0-4 removes only those components that were added through its installation process. The PRS Compatibility Toolkit and PXE PDK, also installed with the Self-Test kit, provide on their own Install and uninstall facilities. Use the appropriate uninstall facility for each tool.

PART 4: RELEASE CHANGES

New Functionality, Enhancements, Bug fixes

There are a number of enhancements to functionality as well as bug fixes. Details of some of these follow in later sections.

Enhancements:

- The installation utility allows the selection of individual test tool components on the target system. Support for Windows* 95, Windows 98, Windows NT* Workstation and Windows NT Server has been enhanced.

- All documentation has been updated and now exists in both a Microsoft Word* 97 and DOS text formats for ease of use. PXE test procedures, Remote Wake-up procedure, and Web links were updated. The main Self-Test kit documentation is supplied in Adobe* .PDF format.

- A new bootdisk directory with DOS test utilities such as SMBIOWFM.EXE, BISTEST1.EXE, ISACPI.EXE, and RLOCKOUT.EXE has been added for users who prefer to use a DOS boot disk during DOS testing. Copy these utilities to your boot disk or add them to your PXE boot image for DOS testing.

- New Remote Lockout test tool beta version r.04.

- New Remote Wake-Up tool version v0.4

Bug Fixes:

- Updated this readme file to include new bug reports and issues found/fixed in the this release of the WfM 2.0 Self Test Toolkit.

- The updated COMPCHK2.EXE tool includes bug fixes and enhancements over previous versions of tool. The .REQ files Desktop2.REQ, Server2.REQ, and Mobile2.REQ have valid date attribute value fields added to prevent infrequent syntax errors when loading these files. Also changed name of the server.REQ file to server2.REQ to be consistent with other file names and reduce confusion with WfM 1.1a file with same name.

- PXE PDK 3.0, build 078 provides bug fixes. Bug fixes in result logging and testing order of PXE API sequences which may have given a false failing result are included. Please refer to the PDK release notes for specifics.

- The PRS Compatibility Toolkit includes bug fixes for the installation program and GUI. The Xfragent.DLL TCPIP packet fix for Windows 98 is also included.

- The SMBIOWFM.EXE tool V1.01 provides support for viewing structures above 1 MB. Additionally erroneous messages about system cache field, reset structure length, memory structure display and display of enclosure structure state related fields as well as some not displayed fields were fixed.

- Updated Remote lockout test tool. Bug fixes include intermittent hangs, improper handling of multiple remote lockout events. The new tool uses BIOS reported event capabilities to test for proper V1.10 implementation. Some V1.0 implementation support was added. Total error count summary added.

- Modified file name on page 13 of WfM 2.0 Self Test Instruction manual. File name SERVER.REQ was referenced. SERVER2.REQ is the new correct file name.

- Fixed Dr. Watson error generated in the Remote Wakeup tool when moving dialog boxes small amounts in rapid succession.

New Functionality:

- The new BIS tool tests for BIS implementations and compatibility with the Boot Integrity Services specification.

- The DCTS2 tool was added to complement COMPCHK2 tool and simplify DMI 2.0 testing.

PART 5: KNOWN ANOMALIES

- PRS Compatibility Toolkit: A bug exists where a fault condition occurs if the user attempts to open a trouble ticket after an invalid IP address or other error occurred during submittal of a new trouble ticket. Please refrain from opening the failing ticket. Instead use the menu File/New/Trouble Ticket to resubmit the ticket using a valid IP address or system name.

- RWU : Remote Wakeup test fails on system booted to DOS by using PXE UNDI test or by manual booting of system. This may occur if the proper TCPIP drivers are not loaded or if a valid, bound IP address is not available on the system under test. Please check to see if the proper driver and binding of the address is done. The user may automatically configure the client system by running the PXE APITEST configuration utility. Running this test will properly configure the drivers and IP address. Be sure to properly set up the APITEST before using it. See the PXE PDK documentation for details.

PART 6: DEPENDENCIES

The following files are required for applications that use the PRS SDK in order for it to function:

PRS-specific installed DLLs

These DLLs are installed as part of the PRS SDK install process.

PRSDK.DLL

XFRAGENT.DLL

MOFCMP.DLL

PRS-required installed DLLs

These DLLs may be installed if they are not already present in your system or older versions are detected.

ATL.DLL

Note: Different versions of ATL.DLL are installed depending on whether your operating system is Windows* 95, Windows 98 or Windows NT*.

MSVCRT.DLL

MSVCP60.DLL

The install includes the redistributable version of REGSVR32.EXE for registering DLLs.

Required System DLLs

The following DLLs are required, but should already be present in a standard installation of Windows or Windows NT. They are not shipped with the WfM Self-Test ToolKit.

MSVCIRT.DLL

SHELL32.DLL

KERNEL32.DLL

USER32.DLL

GDI32.DLL

WSOCK32.DLL

OLEAUT32.DLL

OLE32.DLL

OLEDLG.DLL

COMCTL32.DLL

COMDLG32.DLL

WINSOCK2

Note: An installation of Winsock2 is required for the PRS transfer agent, COMPCHK2, and the Remote Wake-up tools to operate correctly.

COMPCHK2 Required Components

COMPCHK2 requires that a DMI V2.0 compliant service provider is installed to function correctly. The error message "..missing WCDMI.DLL" occurs if a DMI Service Provider is not installed properly and is not running. The WfM1.1a file basesys.REQ is no longer required. Common group information is contained in the new files Server2.REQ, Mobil2.REQ and Desktop2.REQ.

SNMP Tool

SNMP services must be installed on both the server and client and configured correctly for the tool to work. The error message "...missing MGMTAPI.DLL" occurs if SNMP services are missing or not configured correctly. Error messages "...snmp entry point could not be found" occurs or "...procedure entry point

SnmpSvcGetEnterpriseOID could not be found from Dynamic Link library snmpapi.dll." is displayed if SNMP services are not installed and configured correctly.

SMBIOWFM Tool

The test platform must support SMBIOS functionality. See the test system documentation for details or contact your vendor. The new release of the tool provides additional debug information. Tool invocation switches are:

smbiowfm [-d] [-x] where

-d Display debug information to the screen

-x Display a formatted dump of the raw structure table data

PART 7: Common Questions

This new section is provided to assist developers in understanding the new technologies and answer common questions regarding the Self-Test utilities.

Q: What version of SMBIOS is required by Wired for Management 2.0?

A: The Wired for Management Baseline 2.0 requires SMBIOS version 2.2 or later be implemented on the platform (pf02).

Additionally, the following are required:

(pf03) System Boot Status

(pf04) Remote Lockout

(pf07) SM BIOS Data

(pf08) System Network Boot Control

Q: Does implementing SMBIOS 2.3 satisfy the Wired for Management 2.0 BIOS requirements?

A: Partially, yes. SMBIOS 2.3 meets the following requirements:

(pf02) SM BIOS 2.2 or later

(pf03) System Boot Status

(pf07) SM BIOS Data

(pf08) System Network Boot Control

Additionally, (pf04) Remote Lockout, must also be implemented.

Q: The SMBIOS 2.2 specification indicates that some of the fields required by the Wired for Management Baseline 2.0 are "RESERVED for future use". Does implementing the Wired for Management Baseline 2.0 cause my BIOS to be out of compliance with the SMBIOS specification?

A: No, the Wired for Management Baseline 2.0 requirements were developed, with the knowledge of the owners of the SMBIOS specification, specifically to make use of these "reserved" fields. This was done so that there would be no conflicts with other vendor-specific definitions, and the SMBIOS specification could share common definitions with the Wired for Management Baseline.

Q: What are the requirements for Remote Lockout on my system?

A: Remote Lockout is a required component of the Wired for Management 2.0 Baseline specification for desktop, server, and mobile platforms. Remote Lockout for a given feature is required on a given platform if a local lockout mechanism is provided. (e.g. power switch, reset button, mouse, or keyboard functionality) For example, if a system provides a lockout to the power switch then remote lockout functionality is required for the power switch only.

Q: When using the COMPCHK2 tool, the error "ERROR: 3503 (882, 11) Attribute - Illegal value" came up when loading the MASTER.MIF or one of the .REQ files. What does it mean?

A: This error is an infrequent error that may come up on some systems. The value 882, 11 represents the line and column number in the MIF file where the error occurred. This represents the ComponentId group, attribute 5. To fix this, go to the line number and manually edit the date value field with a valid DMI date string. A valid DMI Date string is a 28 octet string with the last 3 octets being 0. See the DMI 2.0 specification for an example. In this version of the toolkit all .REQ files have a valid date string in the date attribute value field.

Q: Is there any special equipment that I need to enable Remote WakeUp on my WfM 2.0 system? How do I run the test?

A: No special equipment is needed. Most new network cards and newer systems with built-in LAN adapters provide Remote WakeUp capability that is enabled by default. In the case of built-in network adapters the adapter is enabled using BIOS. When power is turned off on the system using the power switch, the power supply continues to supply a small power source to the NIC card that allows the system to be remotely booted when instructed. This instruction may come as a formatted message such as a "Magic Packet" message. When this wake-up packet is received, the #PME pin is asserted true and the system powers on.

Run the test by invoking the RWU tool and using the menu select the Wake-up test. Enter the MAC address of the NIC card in the system under test and select OK. The target system if enabled will power on and start the boot sequence. The MAC address is a unique physical address of a NIC card. Please refer to the RWU user guide for more details and capabilities of the tool.

Q: What is RWU and RPO?

A: RWU stands for Remote Wake Up. RPO stands for Remote Power On. RWU is a remote wakeup from sleep states S1, S2, S3 and S4 such as wake-up from Standby mode. RPO is a remote wakeup from a soft power off (S5) state.

Q: When using the COMPCHK2 tool I noticed that basesys.REQ was missing. Also, where can I get the Master.MIF file?

A: Basaesys.REQ is no longer required when using COMPCHK2. The WfM2.0 requirements have changed significantly since WfM1.1a. The required definitions are now included in the files Desktop2.REQ, Mobile2.REQ, and Server2.REQ which represent the defined groups for the desktop, mobile and server implementations of WfM 2.0 respectively.

The file Master.MIF is a file containing all of the standard definitions for DMI 2.0. This file is maintained and owned by the Distributed Management Task Force, Inc (DMTF) organization and is available on their Web site at http://www.dmtf.org. The latest versions of the file can be obtained there. Please refer to the COMPCHK2 guide on how to load and use these files.

Q: When using the COMPCHK2 tool for DMI 2.0 service provider testing, it reported the message "Unable to read the Associated Group Attribute. Check this group in the MIF file for the existence of a table definition." I also saw an error message

'EventGenerator|DMTF^^Security Indication\001' did not pass the Standard Group Conformance Check. What does this mean?

A: To fix the problem remove the ID = for the group. Then add the table definition after the group definition for the EventGenerator|DMTF^^Security Indication\001 group in the system MIF file. The reason for the error is that default values are not used in creating a row for DMI groups. Attribute 5 of this group is the associate group attribute which specifies the event generation group. COMPCHK2 needs to verify that this group exists within the same component as the EventGenerator group. Without a table, COMPCHK2 cannot read the event generator attribute. For example, in the following Event Generation Group, attribute 5 gives the associated group attribute, but when the group is installed into the Service Provider this group will have no rows because these values are only default values.

```
Start Group
        Name = "Event Generation"
        Class = "EventGeneration|DMTF^^Voltage Probe|001"
        ID = 210
        Key = 5

        Start Attribute
                Name = "Event Type"
                ID = 1
                Description = "The type of event that has occurred."
                Access = Read-Only
                Storage = Specific
                Type = Start ENUM
                        1 = "Power Supply Status Change"
                End ENUM
                Value = 1

        End Attribute
        Start Attribute
                Name = "Event Severity"
                ID = 2
                Description = "The severity of this event."
                Access = Read-Only
                Storage = Specific
                Type = Start ENUM
                        1 = "Monitor"
                        2 = "Information"
                        4 = "OK"
                        8 = "Non-Critical"
                        16 = "Critical"
                        32 = "Non-Recoverable"
                End ENUM
                Value = 1
        End Attribute
        Start Attribute
                Name = "Is Event State-Based?"
                ID = 3
                Description = "The value of this attribute determines whether the Event "
                        "being reported is a state-based Event or not. If the value of "
                        "this attribute is TRUE then the Event is "
                        "state-based. Otherwise the Event is not state-based."
                Access = Read-Only
                Storage = Specific
                Type = Start ENUM
                        0 = "False"
```

```
                1 = "True"
            End ENUM
            Value = 1
        End Attribute
        Start Attribute
            Name = "Event State Key"
            ID = 4
            Description = "A unique, single integer key into the EventState group if "
                "this is a state-based Event.  If this is not a state-based "
                "Event then this attribute's value is not defined."
            Access = Read-Only
            Storage = Common
            Type = Integer
            Value = 0
        End Attribute
        Start Attribute
            Name = "Associated Group"
            ID = 5
            Description = "The class name of the group that is associated with the "
                "events defined in this EventGeneration group."
            Access = Read-Only
            Storage = Common
            Type = DisplayString(64)
            Value = "DMTF|Voltage Probe|001"
        End Attribute
        Start Attribute
            Name = "Event System"
            ID = 6
            Description = "The major functional aspect of the product causing the fault."
            Access = Read-Only
            Storage = Specific
            Type = Start ENUM
                0 = "Other"
                1 = "Unknown"
            End ENUM
            Value = 1
        End Attribute
        Start Attribute
            Name = "Event Subsystem"
            ID = 7
            Description = "The minor functional aspect of the product causing the fault."
            Access = Read-Only
            Storage = Specific
            Type = Start ENUM
                0 = "Other"
                1 = "Unknown"
            End ENUM
            Value = 1
        End Attribute
End Group

Start Table
   Name = "Event Generation"
   Class = "EventGeneration|DMTF^^Voltage Probe|001"
   Id = 11111 // Use an available id here
        {,,,,,,}
```

End Table

Q: What is PXE and how is it used?

A: PXE refers to Pre-boot Execution Environment. This technology allows a user to boot a system under test and load an operating system of choice remotely. The PXE tool supplied with the WfM Self-Test Toolkit provides developers with the necessary tools and documentation required to test for PXE compatibility.

Q: What does the SNMP tool do?

A: This tool allows developers to test SNMP functionality as specified in the WfM V2.0 Baseline Specification. SNMP is a type of communication protocol like TCPIP that provides special capabilities. Like the COMPCHK2 tool, the SNMP tool allows for the testing of events or "Traps" that occur as a result of the addition, removal, or modification of a DMI component or group. To "trap" such events, the system under test must be registered to a server to send such notifications and must have local instrumentation capable of generating such events. This capability also involves the use of a DMI to SNMP mapper.

More information can be found at:

http://developer.intel.com/ial/wfm/tools/dmi2snmp/index.htm